(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－315201
（P2000－315201A）
(43)公開日　平成12年11月14日(2000.11.14)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　17/10		Ｇ０６Ｆ　15/31	Ｚ　５Ｂ０５６

審査請求　未請求　請求項の数８　ＯＬ　（全 16 頁）

(21)出願番号　特願平11－124804

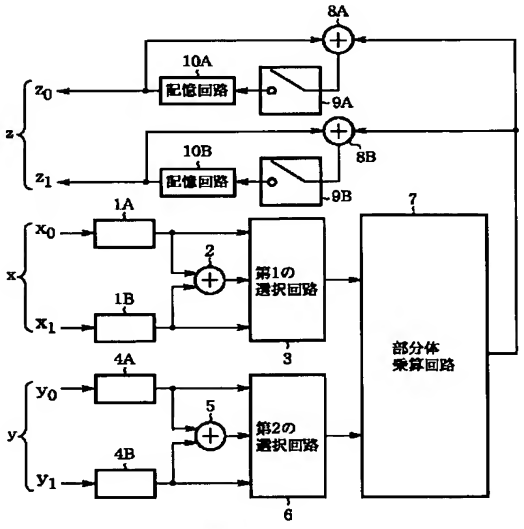
(22)出願日　平成11年４月30日(1999.4.30)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　藤田　八郎
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　吉田　英夫
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100066474
弁理士　田澤　博昭　（外１名）

Ｆターム(参考)　5B056 AA01 AA04 BB00 FF01 FF02 FF05

(54)【発明の名称】　ガロア体乗算回路およびガロア体逆元演算回路

(57)【要約】
【課題】　演算回路全体の回路規模を低減することが困難であった。
【解決手段】　第１の選択回路３は部分体元x_0、部分体元x_1および部分体元x_0，x_1の和のうちのいずれかを選択し、第２の選択回路６は部分体元y_0、部分体元y_1および部分体元y_0，y_1の和のうちのいずれかを選択し、選択された部分体元の積が部分体乗算回路７により演算される。第３および第４の部分体加算回路８Ａ，８Ｂ並びにスイッチ回路９Ａ，９Ｂはそれぞれ所定のタイミングにおいて第３および第４の部分体加算回路８Ａ，８Ｂによる和で、元ｘ，ｙの積ｚに対応する記憶回路１０Ａ，１０Ｂに記憶された部分体の元z_0，z_1を累積更新する。



2：第１の部分体加算回路
5：第２の部分体加算回路
8A：第３の部分体加算回路
8B：第４の部分体加算回路
9A：スイッチ回路（第１の更新回路）
9B：スイッチ回路（第２の更新回路）
10A：記憶回路（第１の記憶回路）
10B：記憶回路（第２の記憶回路）

1

【特許請求の範囲】

【請求項１】　ガロア体の第１の元と第２の元との積を演算するガロア体乗算回路において、

ｎを奇数とするガロア体ＧＦ（2^{2n}）の部分体ＧＦ（2^{n}）の元であって前記ガロア体ＧＦ（2^{2n}）の第１の元に対応する第１の部分体元および第２の部分体元の和を第３の部分体元として演算する第１の部分体加算回路と、

前記部分体の元であって前記ガロア体ＧＦ（2^{2n}）の第２の元に対応する第４の部分体元と第５の部分体元との和を第６の部分体元として演算する第２の部分体加算回路と、

前記第１の部分体元、前記第２の部分体元および前記第３の部分体元のうちのいずれかを選択する第１の選択回路と、

前記第４の部分体元、前記第５の部分体元および前記第６の部分体元のうちのいずれかを選択する第２の選択回路と、

前記第１の選択回路により選択された部分体元と前記第２の選択回路により選択された部分体元との積を演算する部分体乗算回路と、

前記第１の元および前記第２の元の積に対応する前記部分体の２つの元のうちの一方となる前記部分体の元を記憶する第１の記憶回路と、

前記第１の元および前記第２の元の積に対応する前記部分体の２つの元のうちの他方となる前記部分体の元を記憶する第２の記憶回路と、

前記第１の記憶回路に記憶された前記部分体の元と前記部分体乗算回路による積との和を演算する第３の部分体加算回路と、

前記第２の記憶回路に記憶された前記部分体の元と前記部分体乗算回路による積との和を演算する第４の部分体加算回路と、

所定のタイミングにおいて前記第３の部分体加算回路による和で、前記第１の記憶回路に記憶された前記部分体の元を更新する第１の更新回路と、

所定のタイミングにおいて前記第４の部分体加算回路による和で、前記第２の記憶回路に記憶された前記部分体の元を更新する第２の更新回路とを備えることを特徴とするガロア体乗算回路。

【請求項２】　第１の記憶回路および第２の記憶回路は初期値として０を記憶し、

第１の選択回路は、第１のタイミングで第１の部分体元を選択し、第２のタイミングで第２の部分体元を選択し、第３のタイミングで第３の部分体元を選択し、

第２の選択回路は、前記第１のタイミングで第４の部分体元を選択し、前記第２のタイミングで第５の部分体元を選択し、前記第３のタイミングで第６の部分体元を選択し、

第１の更新回路は、前記第１のタイミングおよび前記第２のタイミングで更新し、

第２の更新回路は、前記第１のタイミングおよび前記第３のタイミングで更新することを特徴とする請求項１記載のガロア体乗算回路。

2

【請求項３】　ｎを自然数とし、

第１の選択回路は、第１の部分体元、第２の部分体元、第３の部分体元、およびガロア体ＧＦ（2^{2n}）から部分体ＧＦ（2^{n}）へのノルムである第７の部分体元のうちのいずれかを選択し、

第２の選択回路は、第４の部分体元、第５の部分体元、第６の部分体元、および部分体乗算回路による積のうちのいずれかを選択することを特徴とする請求項１記載のガロア体乗算回路。

【請求項４】　第１の記憶回路および第２の記憶回路は初期値として０を記憶し、

第１の選択回路は、第４のタイミングで第１の部分体元を選択し、第５のタイミングで第２の部分体元を選択した後に第６のタイミングで第７の部分体元を選択し、第７のタイミングで第３の部分体元を選択し、

第２の選択回路は、前記第４のタイミングで第４の部分体元を選択し、前記第５のタイミングで第５の部分体元を選択した後に前記第６のタイミングで、前記第５のタイミングにおける部分体乗算回路による積を選択し、前記第７のタイミングで第６の部分体元を選択し、

第１の更新回路は、前記第４のタイミングおよび前記第６のタイミングで更新し、

第２の更新回路は、前記第４のタイミングおよび前記第７のタイミングで更新することを特徴とする請求項３記載のガロア体乗算回路。

【請求項５】　ガロア体の元の逆元を演算するガロア体逆元演算回路において、

ｎを奇数とするガロア体ＧＦ（2^{2n}）の部分体ＧＦ（2^{n}）の元であって前記ガロア体ＧＦ（2^{2n}）の元に対応する第１の部分体元および第２の部分体元の和を第８の部分体元として演算する第５の部分体加算回路と、

前記第２の部分体元および前記第８の部分体元のうちのいずれかを選択する第３の選択回路と、

前記部分体ＧＦ（2^{n}）の元の逆元を演算する部分体逆元回路と、

前記第１の部分体元、前記第２の部分体元、および前記部分体逆元回路による逆元のうちのいずれかを選択する第４の選択回路と、

前記第３の選択回路により選択された部分体元と前記第４の選択回路により選択された部分体元との積を演算する部分体乗算回路と、

所定のタイミングでの前記部分体乗算回路による積を記憶または累積し、前記部分体逆元回路に供給する記憶累積回路と、

前記部分体ＧＦ（2^{n}）の元であって前記ガロア体ＧＦ（2^{2n}）の元の逆元に対応する第９の部分体元および第

１０の部分体元のうちの前記第９の部分体元として、所定のタイミングにおいて前記部分体乗算回路による積を出力する第１の出力回路と、

前記第１０の部分体元として、所定のタイミングにおいて前記部分体乗算回路による積を出力する第２の出力回路とを備えることを特徴とするガロア体逆元演算回路。

【請求項６】　第３の選択回路は、第８のタイミングで第２の部分体元を選択し、第９のタイミングで第８の部分体元を選択し、第１０のタイミングで第８の部分体元を選択し、第１１のタイミングで第２の部分体元を選択し、

第４の選択回路は、前記第８のタイミングで前記第２の部分体元を選択し、前記第９のタイミングで第１の部分体元を選択し、前記第１０のタイミングおよび第１１のタイミングで部分体逆元回路による逆元を選択し、

記憶累積回路は、前記第８のタイミングで前記部分体乗算回路による積を記憶し、前記第９のタイミングでその記憶した値を前記部分体逆元回路に供給した後に前記部分体乗算回路による積を累積記憶し、前記第１０のタイミングおよび第１１のタイミングでその累積記憶した値を前記部分体逆元回路に供給し、

第１の出力回路は、前記第１０のタイミングで出力し、

第２の出力回路は、前記第１１のタイミングで出力することを特徴とする請求項５記載のガロア体逆元演算回路。

【請求項７】　ｎを自然数とし、

第３の選択回路は、第２の部分体元、第８の部分体元、およびガロア体ＧＦ（2^{2n}）から部分体ＧＦ（2^{n}）へのノルムである第１１の部分体元のうちのいずれかを選択し、

第４の選択回路は、第１の部分体元、第２の部分体元、部分体逆元回路による逆元、および記憶累積回路に記憶または累積された値のうちのいずれかを選択することを特徴とする請求項５記載のガロア体逆元演算回路。

【請求項８】　第３の選択回路は、第１２のタイミングで第２の部分体元を選択し、第１３のタイミングで第１１の部分体元を選択し、第１４のタイミングおよび第１５のタイミングで第８の部分体元を選択し、第１６のタイミングで前記第２の部分体元を選択し、

第４の選択回路は、前記第１２のタイミングで前記第２の部分体元を選択し、前記第１３のタイミングで記憶累積回路の記憶値を選択し、前記第１４のタイミングで第１の部分体元を選択し、前記第１５のタイミングおよび前記第１６のタイミングで部分体逆元回路による逆元を選択し、

記憶累積回路は、前記第１２のタイミングで前記部分体乗算回路による積を記憶し、前記第１３のタイミングでその記憶した値を前記第４の選択回路に供給した後に前記部分体乗算回路による積を記憶し、前記第１４のタイミングで前記部分体乗算回路による積を累積記憶し、前記第１５のタイミングおよび前記第１６のタイミングでその累積記憶した値を前記部分体逆元回路に供給し、

第１の出力回路は、前記第１５のタイミングで出力し、

第２の出力回路は、前記第１６のタイミングで出力することを特徴とする請求項７記載のガロア体逆元演算回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、例えば符号化器や復号化器において、ガロア体の乗算や逆元演算などのガロア体演算を実行するガロア体乗算回路およびガロア体逆元演算回路に関するものである。

【０００２】

【従来の技術】ガロア体の演算は誤り訂正符号の符号化や復号化において必要とされることが多く、様々な演算方法や演算回路が提案されている。特に基礎体ＧＦ（２）上の偶数次ガロア拡大体ＧＦ（2^{2n}）での演算を、その部分体ＧＦ（2^{n}）での演算により実現する方法が、例えば特開平１－１８１２３２号公報、「有限体ＧＦ（2^{2n}）演算回路に関する一検討」（松井ら著、電子情報通信学会信学技報ＩＴ８８－１４）（以下、文献１という）、「ＧＦ（2^{m}）における逆元の高速算法について」（森井、笠原著、電子情報通信学会信学技報ＩＴ８７－２４）および「ＧＦ（2^{m}）における逆元の高速算法について［ＩＩ］」（森井、笠原著、電子情報通信学会信学技報ＩＴ８７－５４）に提案されている。

【０００３】このうちの例えば文献１を参照して、ガロア体ＧＦ（2^{2n}）での演算とその部分体ＧＦ（2^{n}）の演算との関係について説明する。

【０００４】ｎを自然数とするガロア体ＧＦ（2^{2n}）（以下、Ｋという）は部分体ＧＦ（2^{n}）（以下、Ｌという）を包含し、このガロア体Ｋは部分体Ｌの２次拡大体になる。ここで部分体Ｌに属さないガロア体Ｋの元ａを選ぶと、集合｛１，ａ｝は部分体Ｌ上のガロア体Ｋの基底となる。ガロア体Ｋの元ｘは、この基底および部分体Ｌの２つの元x_0，x_1に基づいて$x=x_0+x_1\times a$と一意的に表される。また、元ａは$a^2+T(a)\times a+N(a)=0$なる関係式を満たし、さらにａとしてＴ（ａ）＝１を満たすものを選ぶ。ただし、次のようにＴ（ａ）は元ａのガロア体Ｋから部分体Ｌへのトレースを表し、Ｎ（ａ）はガロア体Ｋの元ａのガロア体Ｋから部分体Ｌへのノルムを表す。

$$T(a)=a+a^{2^n},\quad N(a)=a^{2^{n+1}}$$

【０００５】そしてガロア体Ｋの演算は上述の基底上では部分体Ｌの演算に分解することができる。

【０００６】まず、ガロア体Ｋの元ｘと元ｙとの加算について説明する。上述のように、ガロア体Ｋの元ｘ，ｙを部分体Ｌの元x_0，x_1，y_0，y_1で表すと次に示すようになる。

5

$x = x_0 + x_1 \times a$

$y = y_0 + y_1 \times a$

【０００７】したがってガロア体Ｋの元ｘと元ｙとの加算は、次に示すように、部分体Ｌの加算に分解される。

$x + y = x_0 + y_0 + (x_1 + y_1) \times a$

【０００８】次にガロア体Ｋの元ｘと元ｙとの乗算について説明する。ガロア体Ｋの元ｘ，ｙを同様に部分体Ｌの元x_0，x_1，y_0，y_1で表すと、ガロア体Ｋの元ｘと元ｙとの乗算は、部分体Ｌでの加算、乗算およびノルム倍乗算に分解される。なお、部分体Ｌの元に対する「－１」の乗算は「＋１」の乗算と等価であるため、ガロア体Ｋの元ｘと元ｙとの乗算は次に示すようになる。

$x \times y = x_0 \times y_0 + N(a) \times x_1 \times y_1 + \{(x_0 + x_1) \times (y_0 + y_1) + x_0 \times y_0\} \times a$

【０００９】同様に、ガロア体Ｋの元ｘの逆元x^{-1}は、次に示すように、部分体Ｌでの加算、２乗演算、乗算、逆元演算およびノルム倍乗算により計算される。

$x^{-1} = \{x_0 \times (x_0 + x_1) + N(a) \times x_1^2\}^{-1} \times (x_0 + x_1) + \{x_0 \times (x_0 + x_1) + N(a) \times x_1^2\}^{-1} \times x_1 \times a$

【００１０】このように、ガロア体Ｋでの加算、乗算および逆元演算は、その部分体Ｌでの演算に置き換えることができる。

【００１１】図５は、例えば文献１に記載の従来のガロア体乗算回路を示すブロック図である。図において、１５１Ａ～１５１Ｄはガロア体Ｋの部分体Ｌの２つの元の和をそれぞれ計算する部分体加算回路であり、１５２Ａ～１５２Ｃはガロア体Ｋの部分体Ｌの２つの元の積をそれぞれ計算する部分体乗算回路であり、１５３は所定の基底｛１，ａ｝に基づいて、部分体Ｌの元に、ガロア体Ｋの元ａについてのノルムＮ（ａ）を乗算するノルム乗算回路である。

【００１２】次に動作について説明する。まず、ガロア体Ｋの元ｘに対応する部分体Ｌの２つの元x_0，x_1が部分体加算回路１５１Ａに供給され、ガロア体Ｋの元ｙに対応する部分体Ｌの２つの元y_0，y_1が部分体加算回路１５１Ｂに供給される。また、部分体元x_1，y_1が部分体乗算回路１５２Ａに供給され、部分体元x_0，y_0が部分体乗算回路１５２Ｂに供給される。

【００１３】そして部分体加算回路１５１Ａは、供給された２つの部分体元x_0，x_1の和（$x_0 + x_1$）を計算して部分体乗算回路１５２Ｃに供給し、部分体加算回路１５１Ｂは、供給された２つの部分体元y_0，y_1の和（$y_0 + y_1$）を計算して部分体乗算回路１５２Ｃに供給する。部分体乗算回路１５２Ｃは、供給された部分体元（$x_0 + x_1$），（$y_0 + y_1$）の積（（$x_0 + x_1$）×（$y_0 + y_1$））を計算して部分体加算回路１５１Ｄに供給する。

【００１４】一方、部分体乗算回路１５２Ａは、供給された２つの部分体元x_1，y_1の積（$x_1 \times y_1$）を計算してノルム乗算回路１５３に供給する。ノルム乗算回路１５３は、供給された部分体元（$x_1 \times y_1$）にノルムＮ（ａ）を乗算し、その演算結果（$x_1 \times y_1 \times N(a)$）を部分体加算回路１５１Ｃに供給する。また部分体乗算回路１５２Ｂは、供給された２つの部分体元x_0，y_0の積（$x_0 \times y_0$）を計算して部分体加算回路１５１Ｃ，１５１Ｄに供給する。

【００１５】そして、部分体加算回路１５１Ｃは、供給された２つの部分体（$x_1 \times y_1 \times N(a)$），（$x_0 \times y_0$）の和を計算し、ガロア体Ｋの元ｘ，ｙの積ｚを基底｛１，ａ｝で分解した際（$z = z_0 + z_1 \times a$）の部分体Ｌの元z_0（$= x_0 \times y_0 + x_1 \times y_1 \times N(a)$）として出力する。また、部分体加算回路１５１Ｄは、供給された２つの部分体（（$x_0 + x_1$）×（$y_0 + y_1$）），（$x_0 \times y_0$）の和を計算し、ガロア体Ｋの元ｘ，ｙの積ｚを基底｛１，ａ｝で分解した際（$z = z_0 + z_1 \times a$）の部分体Ｌの元z_1（$= x_0 \times y_0 + (x_0 + x_1) \times (y_0 + y_1)$）として出力する。

【００１６】このようにしてガロア体Ｋの元ｘ，ｙの積ｚが演算される。

【００１７】また、図６は、例えば文献１に記載の従来のガロア体逆元演算回路を示すブロック図である。図において、１６１Ａおよび１６１Ｂはガロア体Ｋの部分体Ｌの２つの元の和をそれぞれ計算する部分体加算回路であり、１６２Ａ～１６２Ｃはガロア体Ｋの部分体Ｌの２つの元の積をそれぞれ計算する部分体乗算回路であり、１６３は部分体Ｌの元の２乗を演算する部分体２乗回路であり、１６４は所定の基底｛１，ａ｝に基づいて、部分体Ｌの元に、ガロア体Ｋの元ａについてのノルムＮ（ａ）を乗算するノルム乗算回路であり、１６５は部分体Ｌの元の逆元を演算する逆元回路である。

【００１８】次に動作について説明する。まず、ガロア体Ｋの元ｘに対応する部分体Ｌの２つの元x_0，x_1が部分体加算回路１６１Ａに供給され、さらに、部分体元x_0が部分体乗算回路１６２Ａに供給され、部分体元x_1が部分体乗算回路１６２Ｃおよび部分体２乗回路１６３に供給される。

【００１９】そして部分体加算回路１６１Ａは、供給された２つの部分体元x_0，x_1の和（$x_0 + x_1$）を計算して部分体乗算回路１６２Ａ，１６２Ｂに供給し、部分体乗算回路１６２Ａは、供給された部分体元x_0と部分体元（$x_0 + x_1$）との積（$x_0 \times (x_0 + x_1)$）を計算して部分体加算回路１６１Ｂに供給する。

【００２０】一方、部分体２乗回路１６３は、供給された部分体元x_1の２乗を計算してノルム乗算回路１６４に供給する。ノルム乗算回路１６４は、供給された部分体元（x_1^2）にノルムＮ（ａ）を乗算し、その演算結果（$x_1^2 \times N(a)$）を部分体加算回路１６１Ｂに供給する。

【００２１】そして、部分体加算回路１６１Ｂは、供給

された２つの部分体（$x_1^2\times N(a)$），（$x_0\times(x_0+x_1)$）の和（$x_0\times(x_0+x_1)+x_1^2\times N(a)$）を計算し、逆元回路１６５に供給する。逆元回路１６５は供給された部分体元（$x_0\times(x_0+x_1)+x_1^2\times N(a)$）の逆元を演算し、部分体乗算回路１６２Ｂ，１６２Ｃに供給する。

【００２２】部分体乗算回路１６２Ｂは、部分体加算回路１６１Ａからの部分体元（x_0+x_1）と逆元回路１６５からの部分体元（$\{x_0\times(x_0+x_1)+x_1^2\times N(a)\}^{-1}$）との積を計算し、ガロア体Ｋの元ｘの逆元ｚを基底｛１，ａ｝で分解した際（$z=z_0+z_1\times a$）の部分体Ｌの元z_0（$=(x_0+x_1)\times\{x_0\times(x_0+x_1)+x_1^2\times N(a)\}^{-1}$）として出力する。

【００２３】同様に、部分体乗算回路１６２Ｃは、供給された部分体元x_1と逆元回路１６５からの部分体元（$\{x_0\times(x_0+x_1)+x_1^2\times N(a)\}^{-1}$）との積を計算し、ガロア体Ｋの元ｘの逆元ｚを基底｛１，ａ｝で分解した際（$z=z_0+z_1\times a$）の部分体Ｌの元z_1（$=x_1\times\{x_0\times(x_0+x_1)+x_1^2\times N(a)\}^{-1}$）として出力する。

【００２４】このようにしてガロア体Ｋの元ｘの逆元ｚが演算される。

【００２５】なお、その他の従来の技術としては、例えば特開平２－２１７０２２号公報、特開平６－３１４９７９号公報、特開平９－３０５５７２号公報に記載のガロア体演算回路がある。

【００２６】

【発明が解決しようとする課題】従来のガロア体乗算回路およびガロア体逆元演算回路は以上のように構成されているので、部分体元のための演算回路が多く必要になり、全体の回路規模を低減することが困難であるなどの課題があった。

【００２７】例えば上述の従来のガロア体乗算回路では、３個の部分体乗算回路、４個の部分体加算回路および１個のノルム乗算回路で構成されており、特に他の部分体演算回路に比較して回路量が多い部分体乗算回路が多く使用されるため、全体での回路規模が大きくなってしまう。また上述の従来のガロア体逆元演算回路では、３個の部分体乗算回路、２個の部分体加算回路、１個の部分体２乗回路、１個のノルム乗算回路および１個の逆元回路で構成されており、部分体乗算回路が多く使用されるため、全体での回路規模が大きくなってしまう。

【００２８】また、部分体演算回路はいずれもＡＮＤ回路とＥＸＯＲ回路で構成される組合せ回路であるため、部分体演算回路を直列／並列に多数接続して構成され、入力から出力までの遅延が大きくなり演算速度を高くすることが困難であるという課題があった。

【００２９】この発明は上記のような課題を解決するためになされたもので、主に部分体乗算回路の数を少なくするようにして、全体での回路規模を低減するとともに、演算速度を高くすることができるガロア体乗算回路およびガロア体逆元演算回路を得ることを目的とする。

【００３０】

【課題を解決するための手段】この発明に係るガロア体乗算回路は、ガロア体ＧＦ（2^{2n}）（ｎは奇数）の部分体ＧＦ（2^n）の元であってガロア体ＧＦ（2^{2n}）の第１の元に対応する第１の部分体元および第２の部分体元の和を第３の部分体元として演算する第１の部分体加算回路と、部分体の元であってガロア体ＧＦ（2^{2n}）の第２の元に対応する第４の部分体元と第５の部分体元との和を第６の部分体元として演算する第２の部分体加算回路と、第１の部分体元、第２の部分体元および第３の部分体元のうちのいずれかを選択する第１の選択回路と、第４の部分体元、第５の部分体元および第６の部分体元のうちのいずれかを選択する第２の選択回路と、第１の選択回路により選択された部分体元と第２の選択回路により選択された部分体元との積を演算する部分体乗算回路と、第１の元および第２の元の積に対応する部分体の２つの元のうちの一方となる部分体の元を記憶する第１の記憶回路と、第１の元および第２の元の積に対応する部分体の２つの元のうちの他方となる部分体の元を記憶する第２の記憶回路と、第１の記憶回路に記憶された部分体の元と部分体乗算回路による積との和を演算する第３の部分体加算回路と、第２の記憶回路に記憶された部分体の元と部分体乗算回路による積との和を演算する第４の部分体加算回路と、所定のタイミングにおいて第３の部分体加算回路による和で、第１の記憶回路に記憶された部分体の元を更新する第１の更新回路と、所定のタイミングにおいて第４の部分体加算回路による和で、第２の記憶回路に記憶された部分体の元を更新する第２の更新回路とを備えるものである。

【００３１】この発明に係るガロア体乗算回路は、第１の記憶回路および第２の記憶回路に初期値として０を記憶し、第１のタイミングで、第１の選択回路が第１の部分体元を選択するとともに第２の選択回路が第４の部分体元を選択し、第１および第２の更新回路が更新をし、第２のタイミングで、第１の選択回路が第２の部分体元を選択するとともに第２の選択回路が第５の部分体元を選択し、第１の更新回路が更新をし、第３のタイミングで、第１の選択回路が第３の部分体元を選択するとともに第２の選択回路が第６の部分体元を選択し、第２の更新回路が更新するようにしたものである。

【００３２】この発明に係るガロア体乗算回路は、ｎを自然数とし、第１の選択回路が第１の部分体元、第２の部分体元、第３の部分体元、およびガロア体ＧＦ（2^{2n}）から部分体ＧＦ（2^n）へのノルムである第７の部分体元のうちのいずれかを選択し、第２の選択回路が第４の部分体元、第５の部分体元、第６の部分体元、および部分体乗算回路による積のうちのいずれかを選択

するようにしたものである。

【００３３】この発明に係るガロア体乗算回路は、第１の記憶回路および第２の記憶回路に初期値として０を記憶し、第４のタイミングで、第１の選択回路が第１の部分体元を選択するとともに第２の選択回路が第４の部分体元を選択し、第１の更新および第２の更新回路が更新をし、第５のタイミングで、第１の選択回路が第２の部分体元を選択し、第２の選択回路が第５の部分体元を選択した後に第６のタイミングで、第１の選択回路が第７の部分体元を選択するとともに第２の選択回路が第５のタイミングにおける部分体乗算回路による積を選択し、第１の更新回路が更新をし、第７のタイミングで、第１の選択回路が第３の部分体元を選択するとともに第２の選択回路が第６の部分体元を選択し、第２の更新回路が更新をするようにしたものである。

【００３４】この発明に係るガロア体逆元演算回路は、ガロア体ＧＦ（2^{2n}）（ｎは奇数）の部分体ＧＦ（2^{n}）の元であってガロア体ＧＦ（2^{2n}）の元に対応する第１の部分体元および第２の部分体元の和を第８の部分体元として演算する第５の部分体加算回路と、第２の部分体元および第８の部分体元のうちのいずれかを選択する第３の選択回路と、部分体ＧＦ（2^{n}）の元の逆元を演算する部分体逆元回路と、第１の部分体元、第２の部分体元、および部分体逆元回路による逆元のうちのいずれかを選択する第４の選択回路と、第３の選択回路により選択された部分体元と第４の選択回路により選択された部分体元との積を演算する部分体乗算回路と、所定のタイミングでの部分体乗算回路による積を記憶または累積し、部分体逆元回路に供給する記憶累積回路と、部分体ＧＦ（2^{n}）の元であってガロア体ＧＦ（2^{2n}）の元の逆元に対応する第９の部分体元および第１０の部分体元のうちの第９の部分体元として所定のタイミングにおいて部分体乗算回路による積を出力する第１の出力回路と、第１０の部分体元として所定のタイミングにおいて部分体乗算回路による積を出力する第２の出力回路とを備えるものである。

【００３５】この発明に係るガロア体逆元演算回路は、第８のタイミングで、第３の選択回路が第２の部分体元を選択するとともに第４の選択回路が第２の部分体元を選択し、記憶累積回路が部分体乗算回路による積を記憶し、第９のタイミングで、第３の選択回路が第８の部分体元を選択するとともに第４の選択回路が第１の部分体元を選択し、記憶累積回路が記憶している値を部分体逆元回路に供給した後に部分体乗算回路による積を累積記憶し、第１０のタイミングで、第３の選択回路が第８の部分体元を選択するとともに第４の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第１の出力回路が出力をし、第１１のタイミングで、第３の選択回路が第２の部分体元を選択するとともに第４の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第２の出力回路が出力をするようにしたものである。

【００３６】この発明に係るガロア体逆元演算回路は、ｎを自然数とし、第３の選択回路が第２の部分体元、第８の部分体元、およびガロア体ＧＦ（2^{2n}）から部分体ＧＦ（2^{n}）へのノルムである第１１の部分体元のうちのいずれかを選択し、第４の選択回路が第１の部分体元、第２の部分体元、部分体逆元回路による逆元、および記憶累積回路に記憶または累積された値のうちのいずれかを選択するようにしたものである。

【００３７】この発明に係るガロア体逆元演算回路は、第１２のタイミングで、第３の選択回路が第２の部分体元を選択するとともに第４の選択回路が第２の部分体元を選択し、記憶累積回路が部分体乗算回路による積を記憶し、第１３のタイミングで、第３の選択回路が第１１の部分体元を選択するとともに第４の選択回路が記憶累積回路の記憶値を選択し、記憶累積回路が記憶している値を第４の選択回路に供給した後に部分体乗算回路による積を記憶し、第１４のタイミングで、第３の選択回路が第８の部分体元を選択するとともに第４の選択回路が第１の部分体元を選択し、記憶累積回路が部分体乗算回路による積を累積記憶し、第１５のタイミングで、第３の選択回路が第８の部分体元を選択するとともに第４の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第１の出力回路が出力をし、第１６のタイミングで、第３の選択回路が第２の部分体元を選択するとともに第４の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第２の出力回路が出力をするようにしたものである。

【００３８】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態１．この発明の実施の形態１によるガロア体乗算回路は、ｎを奇数とするガロア体ＧＦ（2^{2n}）の２つの元ｘ，ｙの積ｚを演算するものである。図１は、この発明の実施の形態１によるガロア体乗算回路の構成を示すブロック図である。

【００３９】図において、１Ａおよび１Ｂは、ｎを奇数とするガロア体ＧＦ（2^{2n}）の部分体ＧＦ（2^{n}）の元であってガロア体ＧＦ（2^{2n}）の元ｘ（第１の元）（＝$x_0+x_1\times\beta$、βは部分体ＧＦ（2^{n}）に属さないガロア体ＧＦ（2^{2n}）の元）に対応する部分体元x_0（第１の部分体元）および部分体元x_1（第２の部分体元）をそれぞれ供給され記憶する記憶回路であり、２は記憶回路１Ａに記憶された部分体元x_0および記憶回路１Ｂに記憶された部分体元x_1の和を演算する第１の部分体加算回路であり、３は記憶回路１Ａに記憶された部分体

元x_0、記憶回路１Ｂに記憶された部分体元x_1および第１の部分体加算回路２の演算結果である部分体元（x_0+x_1）（第３の部分体元）のうちのいずれかを選択する第１の選択回路である。

【００４０】４Ａおよび４Ｂは、ｎを奇数とするガロア体ＧＦ（2^{2n}）の部分体ＧＦ（2^n）の元であってガロア体ＧＦ（2^{2n}）の元ｙ（第２の元）（$=y_0+y_1\times\beta$）に対応する部分体元y_0（第３の部分体元）および部分体元y_1（第４の部分体元）をそれぞれ供給され記憶する記憶回路であり、５は記憶回路４Ａに記憶された部分体元y_0および記憶回路４Ｂに記憶された部分体元y_1の和を演算する第２の部分体加算回路であり、６は記憶回路４Ａに記憶された部分体元y_0、記憶回路４Ｂに記憶された部分体元y_1および第２の部分体加算回路５の演算結果である部分体元（y_0+y_1）（第６の部分体元）のうちのいずれかを選択する第２の選択回路である。

【００４１】７は第１の選択回路３により選択された部分体元と第２の選択回路６により選択された部分体元との積を演算する部分体乗算回路である。８Ａは記憶回路１０Ａに記憶された部分体元と部分体乗算回路７による積との和を演算する第３の部分体加算回路であり、８Ｂは記憶回路１０Ｂに記憶された部分体元と部分体乗算回路７による積との和を演算する第４の部分体加算回路である。９Ａは所定のタイミングにおいてオン状態になり、第３の部分体加算回路８Ａによる和で、記憶回路１０Ａに記憶された部分体元を更新するスイッチ回路（第１の更新回路）であり、９Ｂは所定のタイミングにおいてオン状態になり、第４の部分体加算回路８Ｂによる和で、記憶回路１０Ｂに記憶された部分体元を更新するスイッチ回路（第２の更新回路）である。

【００４２】１０Ａは元ｘおよび元ｙの積ｚ（$=z_0+z_1\times\beta$）に対応する部分体ＧＦ（2^n）の２つの元z_0，z_1のうちの一方（z_0）に最終的になる部分体元を記憶する記憶回路（第１の記憶回路）であり、１０Ｂは元ｘおよび元ｙの積ｚ（$=z_0+z_1\times\beta$）に対応する部分体ＧＦ（2^n）の２つの元z_0，z_1のうちの他方（z_1）に最終的になる部分体元を記憶する記憶回路（第２の記憶回路）である。

【００４３】なお、ｎが奇数である場合、ガロア体ＧＦ（2^{2n}）の上述の元βのノルムＮ（β）は１とすることができるため、元ｘ，ｙの積の演算のためにノルムＮ（β）倍乗算は必要ない。ここで、一例としてｎが７である場合について説明する。ガロア体ＧＦ（2^{14}）の原始多項式を$x^{14}+x^{10}+x^6+x+1$とし、その根（ガロア体ＧＦ（2^{14}）の原始元）をαとする。$\gamma=\alpha^{129}$とおくとγは原始多項式x^7+x+1の根であり、γより生成される部分体はガロア体ＧＦ（2^7）になる。また、$\beta=\alpha^{5461}$とすると、βは部分体ＧＦ（2^7）に属さないためガロア体ＧＦ（2^{14}）はβおよびγにより生成され、集合｛$\beta\gamma^6$，$\beta\gamma^5$，$\beta\gamma^4$，$\beta\gamma^3$，$\beta\gamma^2$，$\beta\gamma$，β，γ^6，γ^5，γ^4，γ^3，γ^2，γ，１｝はガロア体ＧＦ（2^{14}）の基礎体上の基底となる。このとき、$\beta^3=1$なる関係を満たすのでβについてのトレースＴ（β）とノルムＮ（β）は１となる。

【００４４】次に動作について説明する。この実施の形態１によるガロア体乗算回路は、ｎを奇数とするガロア体ＧＦ（2^{2n}）の２つの元ｘ（$=x_0+x_1\times\beta$），ｙ（$=y_0+y_1\times\beta$）の積ｚ（$=z_0+z_1\times\beta$）を３ステップで計算する。

【００４５】まず、記憶回路１Ａ，１Ｂに部分体元x_0，x_1がそれぞれ供給、記憶され、記憶回路４Ａ，４Ｂに部分体元y_0，y_1がそれぞれ供給、記憶され、記憶回路１０Ａ，１０Ｂに初期値０が記憶される。

【００４６】第１のステップ（第１のタイミング）では、スイッチ回路９Ａ，９Ｂがオン状態に制御され、第１の選択回路３が部分体元x_0を選択するとともに第２の選択回路６が部分体元y_0を選択する。したがって部分体乗算回路７に部分体元x_0と部分体元y_0とが供給され、それらの積（$x_0\times y_0$）が部分体乗算回路７により計算され、部分体加算回路８Ａ，８Ｂに供給される。

【００４７】そして、部分体加算回路８Ａ，８Ｂは、記憶回路１０Ａ，１０Ｂに記憶された値（今の場合、初期値０）と部分体乗算回路７による積（$x_0\times y_0$）との和をそれぞれ計算し、スイッチ回路９Ａ，９Ｂを介して記憶回路１０Ａ，１０Ｂにそれぞれ記憶させる。

【００４８】次に第２のステップ（第２のタイミング）では、スイッチ回路９Ａがオン状態に制御されるとともにスイッチ回路９Ｂがオフ状態に制御され、第１の選択回路３が部分体元x_1を選択するとともに第２の選択回路６が部分体元y_1を選択する。したがって部分体乗算回路７に部分体元x_1と部分体元y_1とが供給され、それらの積（$x_1\times y_1$）が部分体乗算回路７により計算され、部分体加算回路８Ａ，８Ｂに供給される。

【００４９】そして、部分体加算回路８Ａ，８Ｂは、記憶回路１０Ａ，１０Ｂに記憶された値（今の場合、$x_0\times y_0$）と部分体乗算回路７による積（$x_1\times y_1$）との和をそれぞれ計算する。今、スイッチ回路９Ａだけがオン状態であるので、部分体加算回路８Ａによる和（$x_0\times y_0+x_1\times y_1$）がスイッチ回路９Ａを介して記憶回路１０Ａに記憶される。なお、記憶回路１０Ｂには、そのまま、部分体元（$x_0\times y_0$）が保持される。

【００５０】最後に第３のステップ（第３のタイミング）では、スイッチ回路９Ａがオフ状態に制御されるとともにスイッチ回路９Ｂがオン状態に制御され、第１の選択回路３が部分体元（x_0+x_1）を選択するとともに第２の選択回路６が部分体元（y_0+y_1）を選択する。したがって部分体乗算回路７に部分体元（x_0+x_1）と部分体元（y_0+y_1）とが供給され、それらの

積（（x_0+x_1）×（y_0+y_1））が部分体乗算回路７により計算され、部分体加算回路８Ａ，８Ｂに供給される。

【００５１】そして、部分体加算回路８Ａは、記憶回路１０Ａに記憶された値（今の場合、（$x_0\times y_0+x_1\times y_1$））と部分体乗算回路７による積（（$x_0+x_1$）×（$y_0+y_1$））との和を計算し、部分体加算回路８Ｂは、記憶回路１０Ｂに記憶された値（今の場合、$x_0\times y_0$）と部分体乗算回路７による積（（x_0+x_1）×（y_0+y_1））との和を計算する。今、スイッチ回路９Ｂだけがオン状態であるので、部分体加算回路８Ｂによる和（$x_0\times y_0$＋（x_0+x_1）×（y_0+y_1））がスイッチ回路９Ｂを介して記憶回路１０Ｂに記憶される。なお、記憶回路１０Ａには、そのまま、部分体元（$x_0\times y_0+x_1\times y_1$）が保持される。

【００５２】このようにして第１～第３のステップの処理により、元ｘおよび元ｙの積ｚ（$=z_0+z_1\times\beta$）に対応する部分体ＧＦ（2^n）の元z_0（$=x_0\times y_0+x_1\times y_1$）が記憶回路１０Ａに記憶され、また出力され、部分体ＧＦ（2^n）の元z_1（$=x_0\times y_0+$（x_0+x_1）×（y_0+y_1））が記憶回路１０Ｂに記憶され、出力される。なお、スイッチ回路９Ａ，９Ｂおよび第１および第２の選択回路３，６の制御は、最終的に記憶回路１０Ａ，１０Ｂに記憶される値が上述のようになれば他の方式でもよい。

【００５３】以上のように、この実施の形態１によれば、ｎが奇数であるガロア体ＧＦ（2^{2n}）についてのガロア体乗算回路における部分体演算回路を１個の部分体乗算回路および４個の部分体加算回路としたので、その他に選択回路、スイッチ回路などが必要になるものの、全体の回路規模を低減することができるという効果が得られる。

【００５４】また、演算を３つのステップに分割し、部分体演算のうち出力遅延の大きい部分体乗算を各ステップにおいて１回だけ実行するようにしたので、乗算全体での出力遅延が低減され、演算を高速に実行することができるという効果が得られる。

【００５５】実施の形態２．この発明の実施の形態２によるガロア体乗算回路は、ｎを自然数とするガロア体ＧＦ（2^{2n}）の２つの元ｘ，ｙの積ｚを演算するものである。図２は、この発明の実施の形態２によるガロア体乗算回路の構成を示すブロック図である。

【００５６】図において、３Ａは記憶回路１Ａに記憶された部分体元x_0、記憶回路１Ｂに記憶された部分体元x_1、第１の部分体加算回路２の演算結果である部分体元（x_0+x_1）および記憶回路２１に記憶されたノルムＮ（β）（第７の部分体元）のうちのいずれかを選択する第１の選択回路である。

【００５７】６Ａは記憶回路４Ａに記憶された部分体元y_0、記憶回路４Ｂに記憶された部分体元y_1、第２の部分体加算回路５の演算結果である部分体元（$=y_0+y_1$）および記憶回路２３に記憶された部分体元のうちのいずれかを選択する第２の選択回路である。

【００５８】２１は元ｘ，ｙと部分体元x_0，x_1，y_0，y_1との対応関係（$x=x_0+x_1\times\beta$，$y=y_0+y_1\times\beta$）を示す部分体ＧＦ（2^n）に属さないガロア体ＧＦ（2^{2n}）の元βについてのガロア体ＧＦ（2^{2n}）から部分体ＧＦ（2^n）へのノルムＮ（β）を供給され記憶する記憶回路であり、２２は部分体乗算回路７による積の供給先を所定のタイミングで切り換えるスイッチ回路であり、２３はスイッチ回路２２を介して供給された部分体乗算回路７による積を記憶する記憶回路である。

【００５９】なお、図２におけるその他の構成要素については実施の形態１によるもの（図１）と同様であるのでその説明を省略する。また、ノルムＮ（β）は図示せぬ所定の演算回路により演算され供給される。

【００６０】なお、ｎが自然数である場合、ガロア体ＧＦ（2^{2n}）の上述の元βのノルムＮ（β）が１とは限らない。ここでｎが４である場合について説明する。ガロア体ＧＦ（2^8）の原始多項式を$x^8+x^6+x^5+x^3+1$とし、その根（ガロア体ＧＦ（2^8）の原始元）をβとする。$\gamma=\beta^{238}$とするとγは原始多項式x^4+x+1の根であり、γより生成される部分体はガロア体ＧＦ（2^4）になる。ガロア体ＧＦ（2^8）はβおよびγより生成され、集合｛$\beta\gamma^3$，$\beta\gamma^2$，$\beta\gamma$，β，γ^3，γ^2，γ，１｝はガロア体ＧＦ（2^8）の基礎体上の基底となる。この場合のノルムＮ（β）はβ^{17}（$=\gamma^{14}$）である。

【００６１】次に動作について説明する。この実施の形態２によるガロア体乗算回路は、ｎを自然数とするガロア体ＧＦ（2^{2n}）の２つの元ｘ（$=x_0+x_1\times\beta$），ｙ（$=y_0+y_1\times\beta$）の積ｚ（$=z_0+z_1\times\beta$）を４ステップで計算する。

【００６２】まず、記憶回路１Ａ，１Ｂに部分体元x_0，x_1がそれぞれ供給、記憶され、記憶回路４Ａ，４Ｂに部分体元y_0，y_1がそれぞれ供給、記憶され、記憶回路２１にノルムＮ（β）が供給、記憶され、記憶回路１０Ａ，１０Ｂに初期値０が記憶される。

【００６３】第１のステップ（第４のタイミング）では、スイッチ回路９Ａ，９Ｂがオン状態に制御されるとともにスイッチ回路２２が部分体乗算回路７と部分体加算回路８Ａ，８Ｂとを電気的に接続し、第１の選択回路３Ａが部分体元x_0を選択するとともに第２の選択回路６Ａが部分体元y_0を選択する。したがって部分体乗算回路７に部分体元x_0と部分体元y_0とが供給され、それらの積（$x_0\times y_0$）が部分体乗算回路７により計算され、スイッチ回路２２を介して部分体加算回路８Ａ，８Ｂに供給される。

15

【００６４】そして、部分体加算回路８Ａ，８Ｂは、記憶回路１０Ａ，１０Ｂに記憶された値（今の場合、初期値０）と部分体乗算回路７による積（$x_0 \times y_0$）との和をそれぞれ計算し、記憶回路１０Ａ，１０Ｂに記憶させる。

【００６５】次に第２のステップ（第５のタイミング）では、スイッチ回路２２が部分体乗算回路７と記憶回路２３とを電気的に接続し、第１の選択回路３Ａが部分体元x_1を選択するとともに第２の選択回路６Ａが部分体元y_1を選択する。したがって部分体乗算回路７に部分体元x_1と部分体元y_1とが供給され、それらの積（$x_1 \times y_1$）が部分体乗算回路７により計算され、スイッチ回路２２を介して記憶回路２３に記憶される。

【００６６】なお、このとき部分体加算回路８Ａ，８Ｂには値が供給されず、記憶回路１０Ａ，１０Ｂに記憶された値（今の場合、$x_0 \times y_0$）はそのまま変化しない。

【００６７】次に第３のステップ（第６のタイミング）では、スイッチ回路９Ａがオン状態に制御されるとともにスイッチ回路９Ｂがオフ状態に制御されるとともに、スイッチ回路２２が部分体乗算回路７と部分体加算回路８Ａ，８Ｂとを電気的に接続し、第１の選択回路３Ａがノルム$N(\beta)$を選択するとともに第２の選択回路６Ａが記憶回路２３に記憶された部分体元（$x_1 \times y_1$）を選択する。したがって部分体乗算回路７にノルム$N(\beta)$と部分体元（$x_1 \times y_1$）とが供給され、それらの積（$N(\beta) \times x_1 \times y_1$）が部分体乗算回路７により計算され、スイッチ回路２２を介して部分体加算回路８Ａ，８Ｂに供給される。

【００６８】そして、部分体加算回路８Ａ，８Ｂは、記憶回路１０Ａ，１０Ｂに記憶された値（今の場合、$x_0 \times y_0$）と部分体乗算回路７による積（$N(\beta) \times x_1 \times y_1$）との和をそれぞれ計算する。今、スイッチ回路９Ａだけがオン状態であるので、部分体加算回路８Ａによる和（$x_0 \times y_0 + N(\beta) \times x_1 \times y_1$）がスイッチ回路９Ａを介して記憶回路１０Ａに記憶される。なお、記憶回路１０Ｂには、そのまま、部分体元（$x_0 \times y_0$）が保持される。

【００６９】最後に第４のステップ（第７のタイミング）では、スイッチ回路９Ａがオフ状態に制御されるとともにスイッチ回路９Ｂがオン状態に制御されるとともにスイッチ回路２２が部分体乗算回路７と部分体加算回路８Ａ，８Ｂとを電気的に接続し、第１の選択回路３Ａが部分体元（$x_0 + x_1$）を選択するとともに第２の選択回路６Ａが部分体元（$y_0 + y_1$）を選択する。したがって部分体乗算回路７に部分体元（$x_0 + x_1$）と部分体元（$y_0 + y_1$）とが供給され、それらの積（（$x_0 + x_1$）×（$y_0 + y_1$））が部分体乗算回路７により計算され、スイッチ回路２２を介して部分体加算回路８Ａ，８Ｂに供給される。

16

【００７０】そして、部分体加算回路８Ａは、記憶回路１０Ａに記憶された値と部分体乗算回路７による積との和を計算し、部分体加算回路８Ｂは、記憶回路１０Ｂに記憶された値（今の場合、$x_0 \times y_0$）と部分体乗算回路７による積（（$x_0 + x_1$）×（$y_0 + y_1$））との和を計算する。今、スイッチ回路９Ｂだけがオン状態であるので、部分体加算回路８Ｂによる和（$x_0 \times y_0 +$（$x_0 + x_1$）×（$y_0 + y_1$））がスイッチ回路９Ｂを介して記憶回路１０Ｂに記憶される。なお、記憶回路１０Ａには、そのまま、部分体元（$x_0 \times y_0 + N(\beta) \times x_1 \times y_1$）が保持される。

【００７１】このようにして第１～第４のステップの処理により、元ｘおよび元ｙの積ｚ（$= z_0 + z_1 \times \beta$）に対応する部分体ＧＦ（2^n）の元z_0（$= x_0 \times y_0 + N(\beta) \times x_1 \times y_1$）が記憶回路１０Ａに記憶され、また出力され、部分体ＧＦ（2^n）の元z_1（$= x_0 \times y_0 +$（$x_0 + x_1$）×（$y_0 + y_1$））が記憶回路１０Ｂに記憶され、出力される。なお、スイッチ回路９Ａ，９Ｂ，２２および第１および第２の選択回路３Ａ，６Ａの制御は、最終的に記憶回路１０Ａ，１０Ｂに記憶される値が上述のようになれば他の方式でもよい。

【００７２】以上のように、この実施の形態２によれば、ｎが自然数であるガロア体ＧＦ（2^{2n}）についてのガロア体乗算回路における部分体演算回路を１個の部分体乗算回路および４個の部分体加算回路としたので、その他に選択回路、スイッチ回路などが必要になるものの、全体の回路規模を低減することができるという効果が得られる。

【００７３】また、演算を４つのステップに分割し、部分体演算のうち出力遅延の大きい部分体乗算を各ステップにおいて１回だけ実行するようにしたので、乗算全体での出力遅延が低減され、演算を高速に実行することができるという効果が得られる。

【００７４】実施の形態３．この発明の実施の形態３によるガロア体逆元演算回路は、ｎを奇数とするガロア体ＧＦ（2^{2n}）の元ｘの逆元ｚ（$= x^{-1}$）を演算するものである。図３は、この発明の実施の形態３によるガロア体逆元演算回路の構成を示すブロック図である。

【００７５】図において、４１Ａおよび４１Ｂは、ｎを奇数とするガロア体ＧＦ（2^{2n}）の部分体ＧＦ（2^n）の元であってガロア体ＧＦ（2^{2n}）の元ｘ（$= x_0 + x_1 \times \beta$、βは部分体ＧＦ（2^n）に属さないガロア体ＧＦ（2^{2n}）の元）に対応する部分体元x_0（第１の部分体元）および部分体元x_1（第２の部分体元）をそれぞれ供給され記憶する記憶回路であり、４２は、記憶回路４１Ａに記憶された部分体元x_0および記憶回路４１Ｂに記憶された部分体元x_1の和（$x_0 + x_1$）を演算する第５の部分体加算回路である。

【００７６】４３は、記憶回路４１Ｂに記憶された部分体元x_1および第５の部分体加算回路４２の演算結果で

ある部分体元（$x_0 + x_1$）（第８の部分体元）のうちのいずれかを選択する第３の選択回路であり、４４は、記憶回路４１Ａに記憶された部分体元x_0、記憶回路４１Ｂに記憶された部分体元x_1および部分体逆元回路５０による逆元のうちのいずれかを選択する第４の選択回路である。

【００７７】４５は、第３の選択回路４３により選択された部分体元と第４の選択回路４４により選択された部分体元との積を演算する部分体乗算回路であり、４６は、部分体乗算回路４５による積の供給先を所定のタイミングで切り換えるスイッチ回路である。

【００７８】４９は所定のタイミングでの部分体乗算回路４５による積を記憶または累積し、部分体逆元回路５０に供給する記憶累積回路である。記憶累積回路４９において、４７は、記憶回路４８に記憶された部分体元と、スイッチ回路４６を介して供給された部分体乗算回路４５による積との和を計算する部分体加算回路であり、４８は部分体加算回路４７の演算結果を記憶する記憶回路である。５０は、記憶回路４８に記憶された部分体元の逆元を演算する部分体逆元回路である。

【００７９】５３Ａは、部分体ＧＦ（2^n）の元であってガロア体ＧＦ（2^{2n}）の元ｘの逆元ｚ（$= z_0 + z_1 \times \beta$）に対応する部分体元z_0（第９の部分体元）として、所定のタイミングにおいてスイッチ回路４６を介して部分体乗算回路４５による積を出力する第１の出力回路である。第１の出力回路５３Ａにおいて、５１Ａは、所定のタイミングにおいてオン状態になり、スイッチ回路４６を介して供給される部分体乗算回路４５による積を記憶回路５２Ａに記憶させるスイッチ回路であり、５２Ａは部分体元z_0を記憶する記憶回路である。

【００８０】５３Ｂは、逆元ｚ（$= z_0 + z_1 \times \beta$）に対応する部分体元z_1（第１０の部分体元）として、所定のタイミングにおいてスイッチ回路４６を介して部分体乗算回路４５による積を出力する第２の出力回路である。第２の出力回路５３Ｂにおいて、５１Ｂは、所定のタイミングにおいてオン状態になり、スイッチ回路４６を介して供給される部分体乗算回路４５による積を記憶回路５２Ｂに記憶させるスイッチ回路であり、５２Ｂは部分体元z_1を記憶する記憶回路である。

【００８１】次に動作について説明する。この実施の形態３によるガロア体逆元演算回路は、ｎを奇数とするガロア体ＧＦ（2^{2n}）の元ｘ（$= x_0 + x_1 \times \beta$）の逆元x^{-1}（$= z = z_0 + z_1 \times \beta$）を４ステップで計算する。

【００８２】まず、記憶回路４１Ａ，４１Ｂに部分体元x_0，x_1がそれぞれ供給、記憶され、記憶累積回路４９の記憶回路４８に初期値０が記憶される。

【００８３】第１のステップ（第８のタイミング）では、スイッチ回路４６が部分体乗算回路４５と記憶累積回路４９とを電気的に接続し、第３の選択回路４３が部分体元x_1を選択するとともに第４の選択回路４４が部分体元x_1を選択する。したがって部分体乗算回路４５に部分体元x_1と部分体元x_1とが供給され、それらの積（x_1^2）が部分体乗算回路４５により計算され、スイッチ回路４６を介して記憶累積回路４９の部分体加算回路４７に供給される。

【００８４】そして、部分体加算回路４７は、記憶回路４８に記憶された値（今の場合、初期値０）と部分体乗算回路４５による積（x_1^2）との和を計算し、記憶回路４８に記憶させる。なお、このとき、第１および第２の出力回路５３Ａ，５３Ｂには値が供給されず特に動作しない。

【００８５】次に第２のステップ（第９のタイミング）では、スイッチ回路４６が部分体乗算回路４５と記憶累積回路４９とを電気的に接続し、第３の選択回路４３が部分体元（$x_0 + x_1$）を選択するとともに第４の選択回路４４が部分体元x_0を選択する。したがって部分体乗算回路４５に部分体元（$x_0 + x_1$）と部分体元x_0とが供給され、それらの積（$x_0 \times (x_0 + x_1)$）が部分体乗算回路４５により計算され、スイッチ回路４６を介して記憶累積回路４９の部分体加算回路４７に供給される。

【００８６】そして、部分体加算回路４７は、記憶回路４８に記憶された値（今の場合、x_1^2）と部分体乗算回路４５による積（$x_0 \times (x_0 + x_1)$）との和（$x_1^2 + x_0 \times (x_0 + x_1)$）を計算し、記憶回路４８に記憶させる。なお、このとき、第１および第２の出力回路５３Ａ，５３Ｂには値が供給されず特に動作しない。

【００８７】次に第３のステップ（第１０のタイミング）では、スイッチ回路４６が部分体乗算回路４５と第１および第２の出力回路５３Ａ，５３Ｂとを電気的に接続し、第１の出力回路５３Ａのスイッチ回路５１Ａがオン状態に制御されるとともに第２の出力回路５３Ｂのスイッチ回路５１Ｂがオフ状態に制御され、第３の選択回路４３が部分体元（$x_0 + x_1$）を選択するとともに、第４の選択回路４４が、記憶累積回路４９に累積記憶している値の部分体逆元回路５０による逆元（今の場合、$\{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$）を選択する。

【００８８】したがって部分体乗算回路４５に部分体元（$x_0 + x_1$）と部分体元（$\{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$）とが供給され、それらの積（$(x_0 + x_1) \times \{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$）が部分体乗算回路４５により計算され、スイッチ回路４６を介して第１および第２の出力回路５３Ａ，５３Ｂに供給される。

【００８９】そして、第１の出力回路５３Ａだけが、その積をスイッチ回路５１Ａを介して記憶回路５２Ａに記憶し、逆元x^{-1}（$= z = z_0 + z_1 \times \beta$）に対応する部分体元$z_0$（$= (x_0 + x_1) \times \{x_1^2 + x_0 \times (x_0 + x_1)\}^{-1}$）として出力する。

【００９０】最後に第４のステップ（第１１のタイミン

グ）では、スイッチ回路４６が部分体乗算回路４５と第１および第２の出力回路５３Ａ，５３Ｂとを電気的に接続し、第１の出力回路５３Ａのスイッチ回路５１Ａがオフ状態に制御されるとともに第２の出力回路５３Ｂのスイッチ回路５１Ｂがオン状態に制御され、第３の選択回路４３が部分体元x_1を選択するとともに第４の選択回路４４が、記憶累積回路４９に累積記憶している値の部分体逆元回路５０による逆元（今の場合、$\{x_1^2+x_0\times(x_0+x_1)\}^{-1}$）を選択する。

【００９１】したがって部分体乗算回路４５に部分体元x_1と部分体元（$\{x_1^2+x_0\times(x_0+x_1)\}^{-1}$）とが供給され、それらの積（$x_1\times\{x_1^2+x_0\times(x_0+x_1)\}^{-1}$）が部分体乗算回路４５により計算され、スイッチ回路４６を介して第１および第２の出力回路５３Ａ，５３Ｂに供給される。

【００９２】そして、第２の出力回路５３Ｂだけが、その積をスイッチ回路５１Ｂを介して記憶回路５２Ｂに記憶し、逆元x^{-1}（$=z=z_0+z_1\times\beta$）に対応する部分体元z_1（$=x_1\times\{x_1^2+x_0\times(x_0+x_1)\}^{-1}$）として出力する。

【００９３】このようにして第１～第４のステップの処理により、第１の出力回路５３Ａにより、元ｘの逆元ｚ（$=z_0+z_1\times\beta$）に対応する部分体ＧＦ（2^n）の元z_0（$=(x_0+x_1)\times\{x_1^2+x_0\times(x_0+x_1)\}^{-1}$）が記憶、出力され、第２の出力回路５３Ｂにより、部分体ＧＦ（2^n）の元z_1（$=x_1\times\{x_1^2+x_0\times(x_0+x_1)\}^{-1}$）が記憶、出力される。なお、スイッチ回路４６，５１Ａ，５１Ｂおよび第３および第４の選択回路４３，４４の制御は、最終的に記憶回路５２Ａ，５２Ｂに記憶される値が上述のようになれば他の方式でもよい。

【００９４】以上のように、この実施の形態３によれば、ｎが奇数であるガロア体ＧＦ（2^{2n}）についてのガロア体逆元演算回路における部分体演算回路を１個の部分体乗算回路、２個の部分体加算回路および１個の部分体逆元回路としたので、その他に選択回路、スイッチ回路などが必要になるものの、全体の回路規模を低減することができるという効果が得られる。

【００９５】また、演算を４つのステップに分割し、部分体演算のうち出力遅延の大きい部分体乗算を各ステップにおいて１回だけ実行するようにしたので、逆元演算全体での出力遅延が低減され、演算を高速に実行することができるという効果が得られる。

【００９６】実施の形態４．この発明の実施の形態４によるガロア体逆元演算回路は、ｎを自然数とするガロア体ＧＦ（2^{2n}）の元ｘの逆元ｚ（$=x^{-1}$）を演算するものである。図４は、この発明の実施の形態４によるガロア体逆元演算回路の構成を示すブロック図である。

【００９７】図において、４３Ａは、記憶回路４１Ｂに記憶された部分体元x_1、部分体加算回路４２による和である部分体元（x_0+x_1）、および記憶回路６１に記憶されたノルムＮ（β）（第１１の部分体元）のうちのいずれかを選択する第３の選択回路である。

【００９８】４４Ａは記憶回路４１Ａに記憶された部分体元x_0、記憶回路４１Ｂに記憶された部分体元x_1、部分体逆元回路５０による逆元、および記憶累積回路４９Ａの記憶回路４８に記憶または累積された値のうちのいずれかを選択する第４の選択回路である。第４の選択回路４４Ａにおいて、６３は、記憶回路４１Ａに記憶された部分体元x_0、記憶回路４１Ｂに記憶された部分体元x_1、選択回路６４により選択された値のうちのいずれかを選択する選択回路であり、６４は、部分体逆元回路５０による逆元、および記憶累積回路４９Ａの記憶回路４８に記憶または累積された値のうちのいずれかを選択する選択回路である。

【００９９】４９Ａは所定のタイミングでの部分体乗算回路４５による積を記憶または累積し、部分体逆元回路５０に供給する記憶累積回路である。記憶累積回路４９Ａにおいて、６２は部分体加算回路４７による和およびスイッチ回路４６を介して供給された部分体乗算回路４５による積のいずれかを選択し、選択した値を記憶回路４８に記憶させる選択回路である。

【０１００】６１は元ｘと部分体元x_0，x_1との対応関係（$x=x_0+x_1\times\beta$）を示す部分体ＧＦ（2^n）に属さないガロア体ＧＦ（2^{2n}）の元βについてのガロア体ＧＦ（2^{2n}）から部分体ＧＦ（2^n）へのノルムＮ（β）を供給され記憶する記憶回路である。

【０１０１】なお、図４におけるその他の構成要素については実施の形態３によるもの（図３）と同様であるのでその説明を省略する。また、ノルムＮ（β）は図示せぬ所定の演算回路により演算され供給される。

【０１０２】次に動作について説明する。この実施の形態４によるガロア体逆元演算回路は、ｎを自然数とするガロア体ＧＦ（2^{2n}）の元ｘ（$=x_0+x_1\times\beta$）の逆元x^{-1}（$=z=z_0+z_1\times\beta$）を５ステップで計算する。例えばｎを４とすると、ガロア体ＧＦ（2^{2n}）がガロア体ＧＦ（2^8）となり、その部分体ＧＦ（2^n）がガロア体ＧＦ（2^4）となる。その場合、実施の形態２と同様のガロア体ＧＦ（2^8）の基底を使用することができる。

【０１０３】まず、記憶回路４１Ａ，４１Ｂに部分体元x_0，x_1がそれぞれ供給、記憶され、記憶回路６１にノルムＮ（β）が供給、記憶され、記憶累積回路４９Ａの記憶回路４８に初期値０が記憶される。

【０１０４】第１のステップ（第１２のタイミング）では、スイッチ回路４６が部分体乗算回路４５と記憶累積回路４９Ａとを電気的に接続し、第３の選択回路４３Ａが部分体元x_1を選択するとともに第４の選択回路４４Ａが部分体元x_1を選択し、選択回路６２は、部分体乗算回路４５による積を選択する。したがって部分体乗算

回路４５に部分体元x_1と部分体元x_1とが供給され、それらの積（x_1^2）が部分体乗算回路４５により計算され、スイッチ回路４６を介して記憶累積回路４９Ａの部分体加算回路４７および選択回路６２に供給される。

【０１０５】そして、部分体加算回路４７は記憶回路４８に記憶された値と部分体乗算回路４５による積との和を計算して選択回路６２に供給するが、今の場合、選択回路６２は部分体乗算回路４５による積（x_1^2）を選択し、記憶回路４８に記憶させる。なお、このとき、第１および第２の出力回路５３Ａ，５３Ｂには値が供給されず特に動作しない。

【０１０６】次に第２のステップ（第１３のタイミング）では、スイッチ回路４６が部分体乗算回路４５と記憶累積回路４９Ａとを電気的に接続し、第３の選択回路４３Ａがノルム$N(\beta)$を選択するとともに第４の選択回路４４Ａが記憶回路４８に記憶された部分体元（今の場合、x_1^2）を選択し、選択回路６２は、部分体乗算回路４５による積を選択する。したがって部分体乗算回路４５にノルム$N(\beta)$と部分体元（x_1^2）とが供給され、それらの積（$N(\beta)\times x_1^2$）が部分体乗算回路４５により計算され、スイッチ回路４６を介して記憶累積回路４９Ａの部分体加算回路４７および選択回路６２に供給される。

【０１０７】そして、部分体加算回路４７は、記憶回路４８に記憶された値と部分体乗算回路４５による積との和を計算して選択回路６２に供給するが、今の場合、選択回路６２は部分体乗算回路４５による積（$N(\beta)\times x_1^2$）を選択し、記憶回路４８に記憶させる。なお、このとき、第１および第２の出力回路５３Ａ，５３Ｂには値が供給されず特に動作しない。

【０１０８】次に第３のステップ（第１４のタイミング）では、スイッチ回路４６が部分体乗算回路４５と記憶累積回路４９Ａとを電気的に接続し、第３の選択回路４３Ａが部分体元（x_0+x_1）を選択するとともに第４の選択回路４４Ａが部分体元x_0を選択し、選択回路６２は、部分体加算回路４７による和を選択する。したがって部分体乗算回路４５に部分体元（x_0+x_1）と部分体元x_0とが供給され、それらの積（（x_0+x_1）$\times x_0$）が部分体乗算回路４５により計算され、スイッチ回路４６を介して記憶累積回路４９Ａの部分体加算回路４７および選択回路６２に供給される。

【０１０９】そして、部分体加算回路４７は記憶回路４８に記憶された値（今の場合、$N(\beta)\times x_1^2$）と部分体乗算回路４５による積（$x_0\times(x_0+x_1)$）との和を計算して選択回路６２に供給し、選択回路６２は、部分体加算回路４７による和（$N(\beta)\times x_1^2+x_0\times(x_0+x_1)$）を選択し、記憶回路４８に記憶させる。なお、このとき、第１および第２の出力回路５３Ａ，５３Ｂには値が供給されず特に動作しない。

【０１１０】次に第４のステップ（第１５のタイミング）では、スイッチ回路４６が部分体乗算回路４５と第１および第２の出力回路５３Ａ，５３Ｂとを電気的に接続し、第１の出力回路５３Ａのスイッチ回路５１Ａがオン状態に制御されるとともに第２の出力回路５３Ｂのスイッチ回路５１Ｂがオフ状態に制御され、第３の選択回路４３Ａが部分体元（x_0+x_1）を選択するとともに第４の選択回路４４Ａが部分体逆元回路５０による逆元（今の場合、$\{N(\beta)\times x_1^2+x_0\times(x_0+x_1)\}^{-1}$）を選択する。

【０１１１】したがって部分体乗算回路４５に部分体元（x_0+x_1）と部分体元（$\{N(\beta)\times x_1^2+x_0\times(x_0+x_1)\}^{-1}$）とが供給され、それらの積（（$x_0+x_1$）$\times\{N(\beta)\times x_1^2+x_0\times(x_0+x_1)\}^{-1}$）が部分体乗算回路４５により計算され、スイッチ回路４６を介して第１および第２の出力回路５３Ａ，５３Ｂに供給される。

【０１１２】そして、第１の出力回路５３Ａだけが、その積をスイッチ回路５１Ａを介して記憶回路５２Ａに記憶し、逆元x^{-1}（$=z=z_0+z_1\times\beta$）に対応する部分体元z_0（$=(x_0+x_1)\times\{N(\beta)\times x_1^2+x_0\times(x_0+x_1)\}^{-1}$）として出力する。

【０１１３】最後に第５のステップ（第１６のタイミング）では、スイッチ回路４６が部分体乗算回路４５と第１および第２の出力回路５３Ａ，５３Ｂとを電気的に接続し、第１の出力回路５３Ａのスイッチ回路５１Ａがオフ状態に制御されるとともに第２の出力回路５３Ｂのスイッチ回路５１Ｂがオン状態に制御され、第３の選択回路４３Ａが部分体元x_1を選択するとともに第４の選択回路４４Ａが、部分体逆元回路５０による逆元（今の場合、$\{N(\beta)\times x_1^2+x_0\times(x_0+x_1)\}^{-1}$）を選択する。

【０１１４】したがって部分体乗算回路４５に部分体元x_1と部分体元（$\{N(\beta)\times x_1^2+x_0\times(x_0+x_1)\}^{-1}$）とが供給され、それらの積（$x_1\times\{N(\beta)\times x_1^2+x_0\times(x_0+x_1)\}^{-1}$）が部分体乗算回路４５により計算され、スイッチ回路４６を介して第１および第２の出力回路５３Ａ，５３Ｂに供給される。

【０１１５】そして、第２の出力回路５３Ｂだけが、その積をスイッチ回路５１Ｂを介して記憶回路５２Ｂに記憶し、逆元x^{-1}（$=z=z_0+z_1\times\beta$）に対応する部分体元z_1（$=x_1\times\{N(\beta)\times x_1^2+x_0\times(x_0+x_1)\}^{-1}$）として出力する。

【０１１６】このようにして第１～第５のステップの処理により、第１の出力回路５３Ａにより、元xの逆元z（$=z_0+z_1\times\beta$）に対応する部分体$GF(2^n)$の元z_0（$=(x_0+x_1)\times\{N(\beta)\times x_1^2+x_0\times(x_0+x_1)\}^{-1}$）が記憶、出力され、第２の出力回路５３Ｂにより、部分体$GF(2^n)$の元z_1（$=x_1\times\{N(\beta)\times x_1^2+x_0\times(x_0+x_1)\}^{-1}$）が記

憶、出力される。なお、スイッチ回路４６，５１Ａ，５１Ｂおよび第３および第４の選択回路４３Ａ，４４Ａの制御は、最終的に記憶回路５２Ａ，５２Ｂに記憶される値が上述のようになれば他の方式でもよい。

【０１１７】以上のように、この実施の形態４によれば、ｎが自然数であるガロア体ＧＦ（2^{2n}）についてのガロア体逆元演算回路における部分体演算回路を１個の部分体乗算回路、２個の部分体加算回路および１個の部分体逆元回路としたので、その他に選択回路、スイッチ回路などが必要になるものの、全体の回路規模を低減することができるという効果が得られる。

【０１１８】また、演算を５つのステップに分割し、部分体演算のうち出力遅延の大きい部分体乗算を各ステップにおいて１回だけ実行するようにしたので、逆元演算全体での出力遅延が低減され、演算を高速に実行することができるという効果が得られる。

【０１１９】

【発明の効果】以上のように、この発明によれば、ガロア体ＧＦ（2^{2n}）（ｎは奇数）の部分体ＧＦ（2^{n}）の元であってガロア体ＧＦ（2^{2n}）の第１の元に対応する第１の部分体元および第２の部分体元の和を第３の部分体元として演算する第１の部分体加算回路と、部分体の元であってガロア体ＧＦ（2^{2n}）の第２の元に対応する第４の部分体元と第５の部分体元との和を第６の部分体元として演算する第２の部分体加算回路と、第１の部分体元、第２の部分体元および第３の部分体元のうちのいずれかを選択する第１の選択回路と、第４の部分体元、第５の部分体元および第６の部分体元のうちのいずれかを選択する第２の選択回路と、第１の選択回路により選択された部分体元と第２の選択回路により選択された部分体元との積を演算する部分体乗算回路と、第１の元および第２の元の積に対応する部分体の２つの元のうちの一方となる部分体の元を記憶する第１の記憶回路と、第１の元および第２の元の積に対応する部分体の２つの元のうちの他方となる部分体の元を記憶する第２の記憶回路と、第１の記憶回路に記憶された部分体の元と部分体乗算回路による積との和を演算する第３の部分体加算回路と、第２の記憶回路に記憶された部分体の元と部分体乗算回路による積との和を演算する第４の部分体加算回路と、所定のタイミングにおいて第３の部分体加算回路による和で第１の記憶回路に記憶された部分体の元を更新する第１の更新回路と、所定のタイミングにおいて第４の部分体加算回路による和で第２の記憶回路に記憶された部分体の元を更新する第２の更新回路とで構成するようにしたので、全体の回路規模を低減することができるという効果がある。

【０１２０】この発明によれば、第１の記憶回路および第２の記憶回路に初期値として０が記憶され、第１のタイミングで、第１の選択回路が第１の部分体元を選択するとともに第２の選択回路が第４の部分体元を選択し、

第１および第２の更新回路が更新をし、第２のタイミングで、第１の選択回路が第２の部分体元を選択するとともに第２の選択回路が第５の部分体元を選択し、第１の更新回路が更新をし、第３のタイミングで、第１の選択回路が第３の部分体元を選択するとともに第２の選択回路が第６の部分体元を選択し、第２の更新回路が更新するようにしたので、乗算全体での出力遅延が低減され、演算を高速に実行することができるという効果がある。

【０１２１】この発明によれば、ｎを自然数とするガロア体ＧＦ（2^{2n}）について、第１の選択回路が第１の部分体元、第２の部分体元、第３の部分体元、およびガロア体ＧＦ（2^{2n}）から部分体ＧＦ（2^{n}）へのノルムである第７の部分体元のうちのいずれかを選択し、第２の選択回路が第４の部分体元、第５の部分体元、第６の部分体元、および部分体乗算回路による積のうちのいずれかを選択するようにしたので、全体の回路規模を低減することができるという効果がある。

【０１２２】この発明によれば、第１の記憶回路および第２の記憶回路に初期値として０が記憶され、第４のタイミングで、第１の選択回路が第１の部分体元を選択するとともに第２の選択回路が第４の部分体元を選択し、第１の更新および第２の更新回路が更新をし、第５のタイミングで、第１の選択回路が第２の部分体元を選択し、第２の選択回路が第５の部分体元を選択した後に第６のタイミングで、第１の選択回路が第７の部分体元を選択するとともに第２の選択回路が第５のタイミングにおける部分体乗算回路による積を選択し、第１の更新回路が更新をし、第７のタイミングで、第１の選択回路が第３の部分体元を選択するとともに第２の選択回路が第６の部分体元を選択し、第２の更新回路が更新をするようにしたので、乗算全体での出力遅延が低減され、演算を高速に実行することができるという効果がある。

【０１２３】この発明によれば、ガロア体ＧＦ（2^{2n}）（ｎは奇数）の部分体ＧＦ（2^{n}）の元であってガロア体ＧＦ（2^{2n}）の元に対応する第１の部分体元および第２の部分体元の和を第８の部分体元として演算する第５の部分体加算回路と、第２の部分体元および第８の部分体元のうちのいずれかを選択する第３の選択回路と、部分体ＧＦ（2^{n}）の元の逆元を演算する部分体逆元回路と、第１の部分体元、第２の部分体元、および部分体逆元回路による逆元のうちのいずれかを選択する第４の選択回路と、第３の選択回路により選択された部分体元と第４の選択回路により選択された部分体元との積を演算する部分体乗算回路と、所定のタイミングでの部分体乗算回路による積を記憶または累積し、部分体逆元回路に供給する記憶累積回路と、部分体ＧＦ（2^{n}）の元であってガロア体ＧＦ（2^{2n}）の元の逆元に対応する第９の部分体元および第１０の部分体元のうちの第９の部分体元として所定のタイミングにおいて部分体乗算回路による積を出力する第１の出力回路と、第１０の部分体元と

して所定のタイミングにおいて部分体乗算回路による積を出力する第２の出力回路とで構成するようにしたので、全体の回路規模を低減することができるという効果がある。

【０１２４】この発明によれば、第８のタイミングで、第３の選択回路が第２の部分体元を選択するとともに第４の選択回路が第２の部分体元を選択し、記憶累積回路が部分体乗算回路による積を記憶し、第９のタイミングで、第３の選択回路が第８の部分体元を選択するとともに第４の選択回路が第１の部分体元を選択し、記憶累積回路が記憶している値を部分体逆元回路に供給した後に部分体乗算回路による積を累積記憶し、第１０のタイミングで、第３の選択回路が第８の部分体元を選択するとともに第４の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第１の出力回路が出力をし、第１１のタイミングで、第３の選択回路が第２の部分体元を選択するとともに第４の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第２の出力回路が出力をするようにしたので、逆元演算全体での出力遅延が低減され、演算を高速に実行することができるという効果がある。

【０１２５】この発明によれば、ｎを自然数とするガロア体ＧＦ（2^{2n}）について、第３の選択回路が第２の部分体元、第８の部分体元、およびガロア体ＧＦ（2^{2n}）から部分体ＧＦ（2^{n}）へのノルムである第１１の部分体元のうちのいずれかを選択し、第４の選択回路が第１の部分体元、第２の部分体元、部分体逆元回路による逆元、および記憶累積回路に記憶または累積された値のうちのいずれかを選択するようにしたので、全体の回路規模を低減することができるという効果がある。

【０１２６】この発明によれば、第１２のタイミングで、第３の選択回路が第２の部分体元を選択するとともに第４の選択回路が第２の部分体元を選択し、記憶累積回路が部分体乗算回路による積を記憶し、第１３のタイミングで、第３の選択回路が第１１の部分体元を選択するとともに第４の選択回路が記憶累積回路の記憶値を選択し、記憶累積回路が記憶している値を第４の選択回路に供給した後に部分体乗算回路による積を記憶し、第１

４のタイミングで、第３の選択回路が第８の部分体元を選択するとともに第４の選択回路が第１の部分体元を選択し、記憶累積回路が部分体乗算回路による積を累積記憶し、第１５のタイミングで、第３の選択回路が第８の部分体元を選択するとともに第４の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第１の出力回路が出力をし、第１６のタイミングで、第３の選択回路が第２の部分体元を選択するとともに第４の選択回路が部分体逆元回路による逆元を選択し、記憶累積回路が累積記憶している値を部分体逆元回路に供給し、第２の出力回路が出力をするようにしたので、逆元演算全体での出力遅延が低減され、演算を高速に実行することができるという効果がある。

【図面の簡単な説明】

【図１】　この発明の実施の形態１によるガロア体乗算回路の構成を示すブロック図である。

【図２】　この発明の実施の形態２によるガロア体乗算回路の構成を示すブロック図である。

【図３】　この発明の実施の形態３によるガロア体逆元演算回路の構成を示すブロック図である。

【図４】　この発明の実施の形態４によるガロア体逆元演算回路の構成を示すブロック図である。

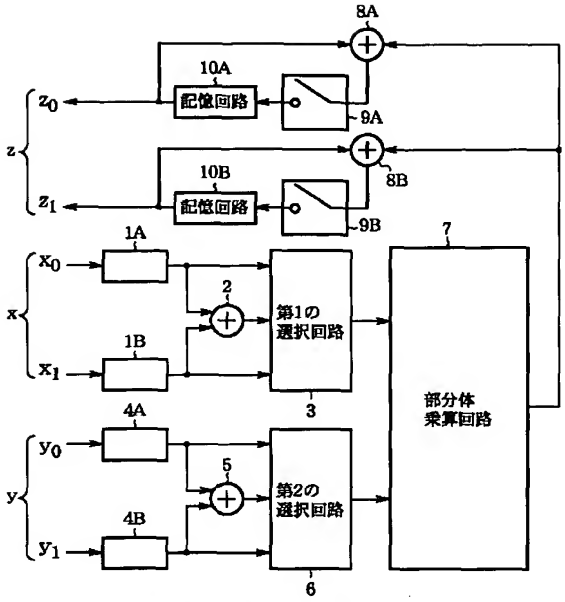
【図５】　従来のガロア体乗算回路を示すブロック図である。

【図６】　従来のガロア体逆元演算回路を示すブロック図である。

【符号の説明】

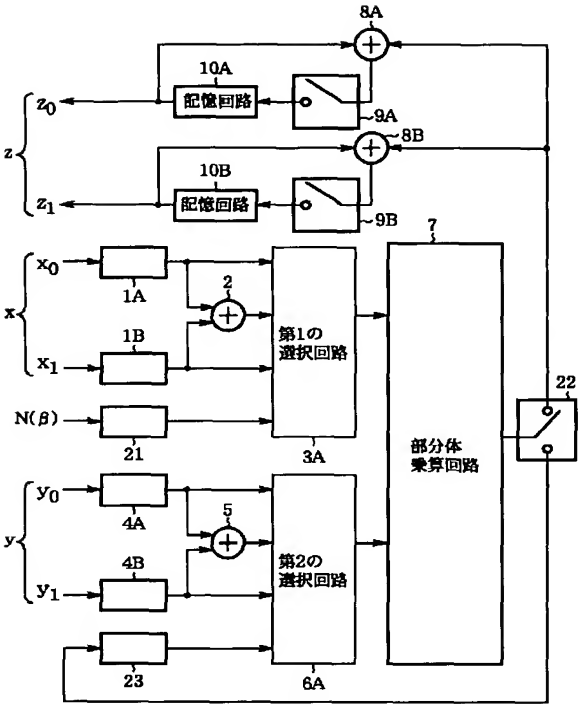
２　第１の部分体加算回路、３，３Ａ　第１の選択回路、５　第２の部分体加算回路、６，６Ａ　第２の選択回路、７　部分体乗算回路、８Ａ　第３の部分体加算回路、８Ｂ　第４の部分体加算回路、９Ａ　スイッチ回路（第１の更新回路）、９Ｂ　スイッチ回路（第２の更新回路）、１０Ａ　記憶回路（第１の記憶回路）、１０Ｂ　記憶回路（第２の記憶回路）、４２　第５の部分体加算回路、４３，４３Ａ　第３の選択回路、４４，４４Ａ　第４の選択回路、４５　部分体乗算回路、５０　部分体逆元回路、５３Ａ　第１の出力回路、５３Ｂ　第２の出力回路。

【図１】

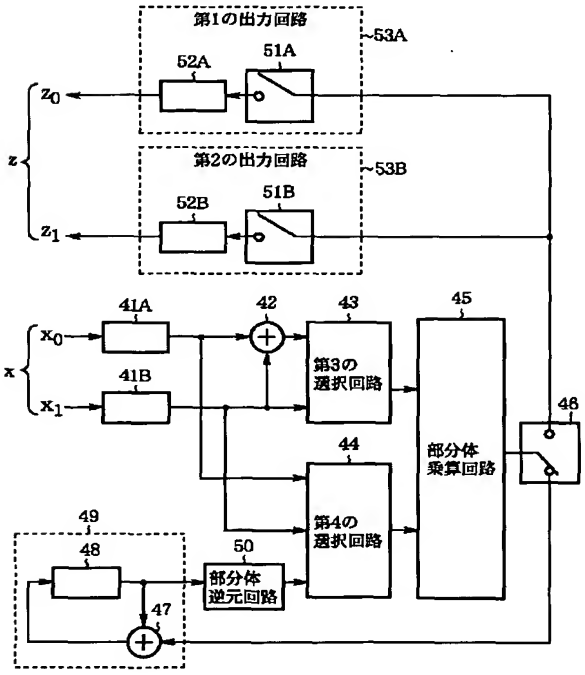


2：第１の部分体加算回路
5：第２の部分体加算回路
8A：第３の部分体加算回路
8B：第４の部分体加算回路
9A：スイッチ回路（第１の更新回路）
9B：スイッチ回路（第２の更新回路）
10A：記憶回路（第１の記憶回路）
10B：記憶回路（第２の記憶回路）

【図２】

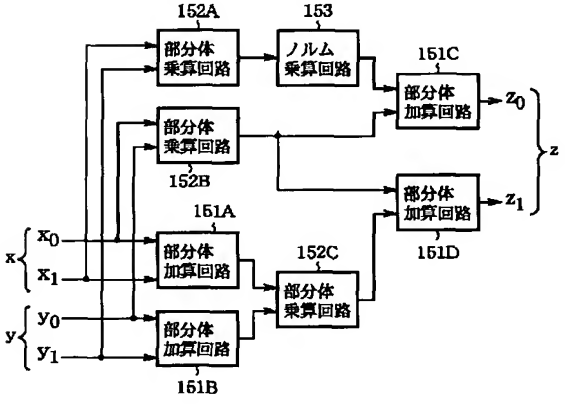


【図３】

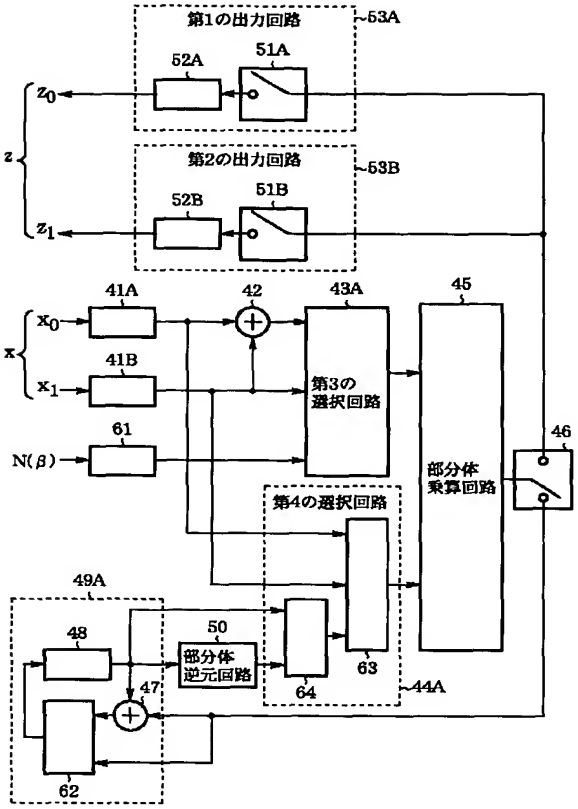


42：第5の部分体加算回路

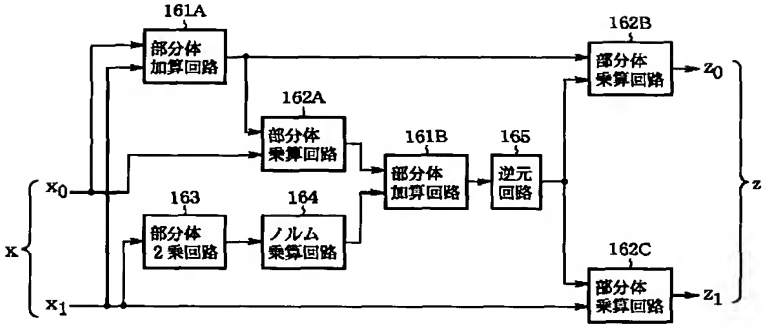
【図５】



【図４】


第1の出力回路
53A
52A
51A
z_0
z
第2の出力回路
53B
52B
51B
z_1
41A
42
43A
45
x_0
x
41B
x_1
第3の
選択回路
61
$N(\beta)$
46
部分体
乗算回路
第4の選択回路
49A
48
50
部分体
逆元回路
47
63
64
44A
62

【図６】


161A
部分体
加算回路
162B
部分体
乗算回路
z_0
162A
部分体
乗算回路
161B
165
部分体
加算回路
逆元
回路
z
x_0
x
163
164
部分体
2乗回路
ノルム
乗算回路
162C
部分体
乗算回路
z_1
x_1